

Web Development Foundations

HTTP cookies. Web sessions.

Assoc. Prof. Andrei PANU – profs.info.uaic.ro/andrei.panu/

* many thanks to Prof. Sabin-Corneliu Buraga for the content on these slides



Table of Contents

1. How can data sent from the server by the Web application be stored at the browser's level
2. How can we identify successive requests sent by the same instance of the client

Is there a way to – temporarily – store
on front-end (browser)
data transmitted by the back-end of a Web application?

Cookies

A script running on a Web server can put data on the client-computer via the user's Web browser

subsequently, the navigator will return that data to the same script available on the same server

Cookies

A (quasi-)persistent way to store data
on the machine of a Web client
in order to be further accessed by a program running on a server

developer.mozilla.org/docs/Web/HTTP/Cookies

also consult Cookiepedia: cookiepedia.co.uk

Cookies – Usages

Storing user preferences

typical examples:

options regarding interaction – visual theme
(e.g., chromatics, graphic arrangement), language preferences,
geographical location, interests on shopping,...

Cookies – Usages

Automatic form completion

using values previously entered by the user
in certain fields

Cookies – Usages

Monitoring the access to a Web resource

aspect of interest:

Web analytics

collecting information about clients

(hardware platform, browser, screen resolution, etc.)

Cookies – Usages

Monitoring the access to a Web resource

aspect of interest:

user tracking

monitoring the user's behavior

-> **Do Not Track initiative**

www.eff.org/issues/do-not-track

Cookies – Usages

Storing authentication info

e.g., keeping data about the user account
in the e-commerce context

Cookies – Usages

Storing authentication info

 never store the user's password

Cookies – Usages

Transaction status

example:

current state of the virtual shopping cart
provided by an e-shop application

Cookies – Usages

Web session management

Cookies – Types

Persistent cookies

not destroyed when the Web browser closes

kept into a file – on the client-side

lifetime set by the cookie creator

Cookies – Types

Non-persistent (volatile) cookies

disappear when the browser is closed

Cookies

a cookie can be considered as a variable

its value is transferred via HTTP
between the Web server (back-end application)
and the client (browser)

the size of a cookie cannot exceed 4KB

Cookies

a cookie can be considered as a variable

name=value

the value is an URL encoded string

Cookies

Data about a cookie is received by the browser

a list of cookies for each server (domain)

Cookies

Data about a cookie is received by the browser

a list of cookies for each server (domain)

1 st party cookies	created by the Web application, belonging to the visited primary domain – (non)persistent [essential or not]
3 rd party cookies	created by external applications – (non)persistent [can cause security problems – privacy]
session cookies	specific to the current Web session – nonpersistent [usually, essential]

Cookies

A cookie is sent to a client
by using the **Set-Cookie**
header field of an HTTP response message

Cookies

```
Set-Cookie: name=value; expires=date; path=path;  
            domain=Internet-domain; secure
```

Cookies

```
Set-Cookie: name=value; expires=date; path=path;  
            domain=Internet-domain; secure
```

expires – indicates the date and time when the cookie will expire
(the Web client should destroy expired cookies)

Cookies

```
Set-Cookie: name=value; expires=date; path=path;  
domain=Internet-domain; secure
```

domain – signifies the symbolic name of the Web server that generated the cookie

Cookies

```
Set-Cookie: name=value; expires=date; path=path;  
domain=Internet-domain; secure
```

path – specifies a subset of URLs
from the cookie's domain

distinguishes multiple applications
existing on the same server

Cookies

```
Set-Cookie: name=value; expires=date; path=path;  
            domain=Internet-domain; secure
```

secure – indicates that the cookie will be sent back to the server only if the communication channel is secure (via HTTPS)

Cookies

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application Hints

Cache Storage Cookies Indexed DB Local Storage Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
__Secure-R...	COHlvDtnZTTeBD4t6WF9dGLA...	.youtube.com	/	Sat, 06 Sep 2025 12:...	66	true	true	None	Mon, 10 Mar 2025 1...
PREF	f4=4000000	.youtube.com	/	Fri, 27 Mar 2026 09:...	14	false	true	None	Mon, 10 Mar 2025 1...
VISITOR_INF...	A89EHRd8o3g	.youtube.com	/	Sat, 06 Sep 2025 12:...	29	true	true	None	Mon, 10 Mar 2025 1...
VISITOR_PRI...	CgJSTxlcEhgSFhMLFBUWFwwY...	.youtube.com	/	Sat, 06 Sep 2025 12:...	76	true	true	None	Mon, 10 Mar 2025 1...
YSC	AE03RGCuyiw	.youtube.com	/	Session	14	true	true	None	Mon, 10 Mar 2025 1...

Filter values

Data

PREF:"f4=4000000"

Created:"Thu, 20 Feb 2025 09:15:28 GMT"

Domain:".youtube.com"

Expires / Max-Age:"Fri, 27 Mar 2026 09:15:28 GMT"

HostOnly:false

HttpOnly:false

Last Accessed:"Mon, 10 Mar 2025 12:48:10 GMT"

Partition Key:"https://google.com"

Path:"/"

SameSite:"None"

Secure:true

Size:14

inspecting cookies stored by the Web browser
for each domain

Cookies

advanced

The screenshot shows the Chrome DevTools Storage tab. The left sidebar lists domains: https://accounts.google.com, https://ogs.google.com, https://www.google.com, and https://www.youtube.com (selected). The main area displays a table of cookies for the selected domain.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
__Secure-R...	COHlvDtnZTTeBD4t6WF9dGLA...	.youtube.com	/	Sat, 06 Sep 2025 12:...	66	true	true	None	Mon, 10 Mar 2025 1...
PREF	f4=4000000	.youtube.com	/	Fri, 27 Mar 2026 09:...	14	false	true	None	Mon, 10 Mar 2025 1...
VISITOR_INF...	A89EHRd8o3g	.youtube.com	/	Sat, 06 Sep 2025 12:...	29	true	true	None	Mon, 10 Mar 2025 1...
VISITOR_PRI...	CgJSTxlcEhgSFhMLFBUWFwwY...	.youtube.com	/	Sat, 06 Sep 2025 12:...	76	true	true	None	Mon, 10 Mar 2025 1...
YSC	AE03RGcuyiw	.youtube.com	/	Session	14	true	true	None	Mon, 10 Mar 2025 1...

The right pane shows the details for the selected 'PREF' cookie:

- Created: "Thu, 20 Feb 2025 09:15:28 GMT"
- Domain: ".youtube.com"
- Expires / Max-Age: "Fri, 27 Mar 2026 09:15:28 GMT"
- HostOnly: false
- HttpOnly: false
- Last Accessed: "Mon, 10 Mar 2025 12:48:10 GMT"
- Partition Key: "https://google.com"
- Path: "/"
- SameSite: "None"
- Secure: true
- Size: 14

inspecting cookies stored by the Web browser
for each domain

httpOnly: true – indicates that the value of a cookie can be obtained
only from a data transfer through HTTP

the cookie cannot be accessed by a program executed on client side (browser) –
owasp.org/www-community/HttpOnly

Cookies

advanced

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Data
vp	1450x160	.emag.ro	/	Tue, 10 Mar 2026 12:39:07 GMT	10	false	false	None	
user_token	63bed597fa14381275290...	.emag.ro	/	Tue, 10 Mar 2026 12:41:27 GMT	42	false	false	None	
user_remember	%DB%11b%C5dy%B9%B...	.emag.ro	/	Tue, 10 Mar 2026 12:41:27 GMT	437	true	true	None	
token1	%2225068527467932800...	.emag.ro	/	Wed, 18 Jun 2025 12:40:18 GMT	92	false	false	None	
sr	2112x1148	.emag.ro	/	Tue, 10 Mar 2026 12:39:07 GMT	11	false	false	None	
site_version_11	not_mobile	.emag.ro	/	Wed, 09 Apr 2025 13:05:53 GMT	25	false	false	None	
sapi-token	eyJ1c2VyX2lkjjoyNTA2OD...	.emag.ro	/	Tue, 10 Mar 2026 12:41:27 GMT	890	false	true	None	
ltuid	2506845546157962524	.emag.ro	/	Tue, 14 Apr 2026 12:39:06 GMT	24	false	false	None	
loginTooltipSho...	1	.emag.ro	/	Tue, 10 Mar 2026 12:39:07 GMT	18	false	false	None	loginTooltipShown:"1" Created:"Mon, 10 Mar 2025 12:39:07 GMT" Domain:".emag.ro" Expires / Max-Age:"Tue, 10 Mar 2026 12:39:07 GMT" HostOnly:false HttpOnly:false Last Accessed:"Mon, 10 Mar 2025 13:05:51 GMT" Path:"/" SameSite:"None" Secure:false Size:18
listingResetView	1	www.emag.ro	/	Tue, 10 Mar 2026 13:05:52 GMT	17	false	false	None	
EMAGVISITOR	a%3A1%3A%7Bs%3A7%3...	.emag.ro	/	Tue, 14 Apr 2026 12:40:18 GMT	75	false	false	None	
EMAGUUID	1741610346-7010970270...	.emag.ro	/	Tue, 14 Apr 2026 12:39:06 GMT	39	false	false	None	
EMAGROSESSID	0ebioaui47e200lqn6np6n...	.emag.ro	/	Tue, 11 Mar 2025 01:05:53 GMT	38	true	true	Lax	
eab_allocation		.emag.ro	/	Mon, 10 Mar 2025 13:06:53 GMT	14	false	false	None	

inspecting cookies stored by the Web browser
for each domain

sameSite – specifies whether the cookie's value
will be passed across requests between different websites
(cross-site requests)

possible values: Strict / Lax / None

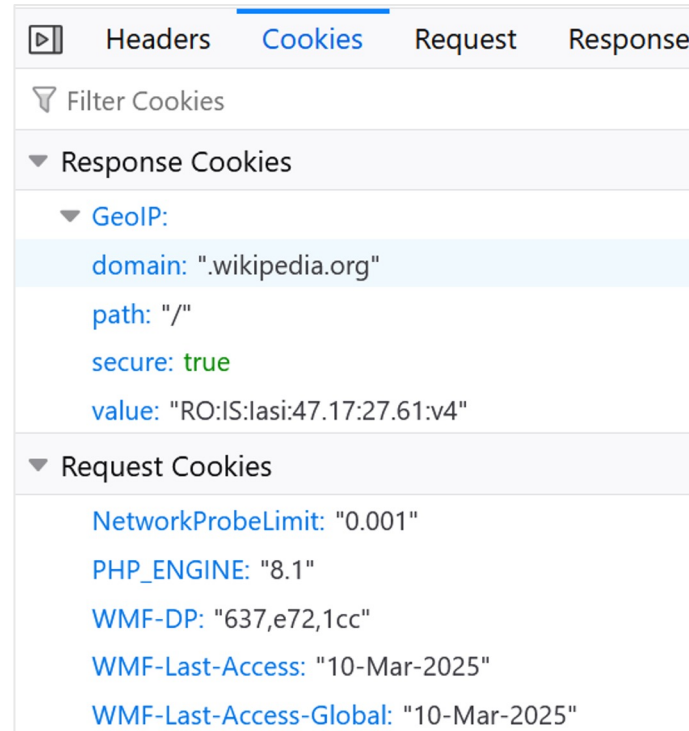
Cookies

A cookie is transmitted back from the client to the Web server only if it satisfies all validity conditions

domain, (virtual) path, expiration time, and communication channel security are matching

Cookies

inspecting the cookies stored by the browser for each domain specific to a Web application



cookie values sent back to the web server
on the next HTTP request

Cookies

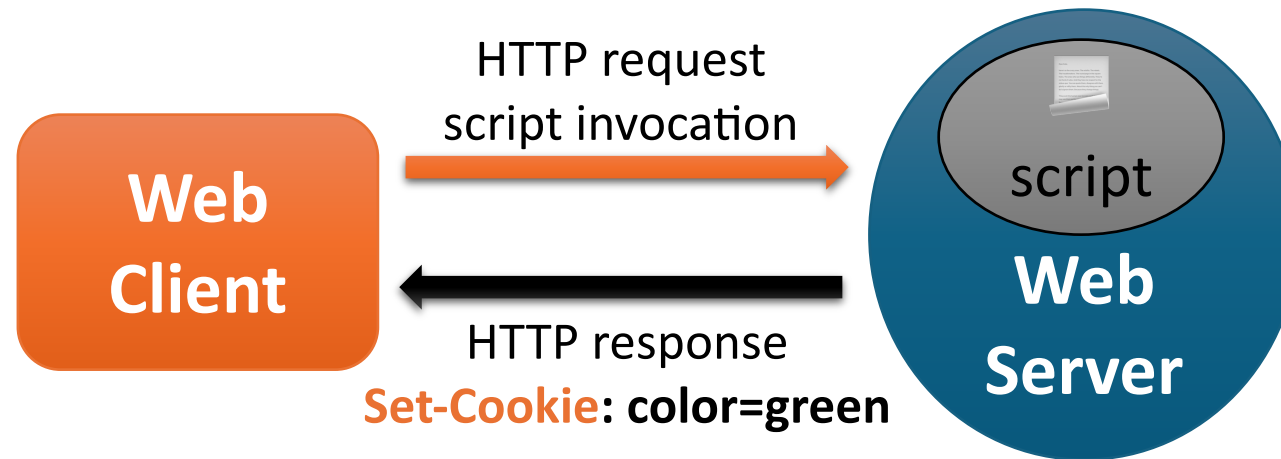
the server will receive, in the header of an HTTP request message, the following:

```
Cookie: name1=value1; name2=value2...
```

the list of cookies which satisfy the validity conditions

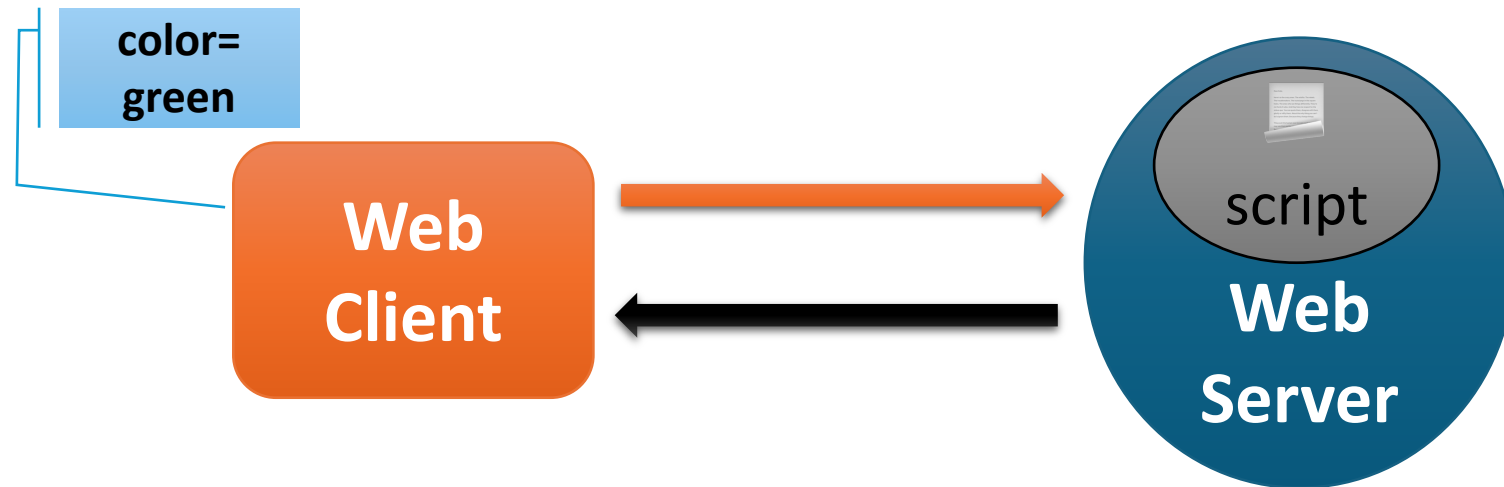
Cookies

A script invocation leads to returning a representation + placing various cookies



Cookies

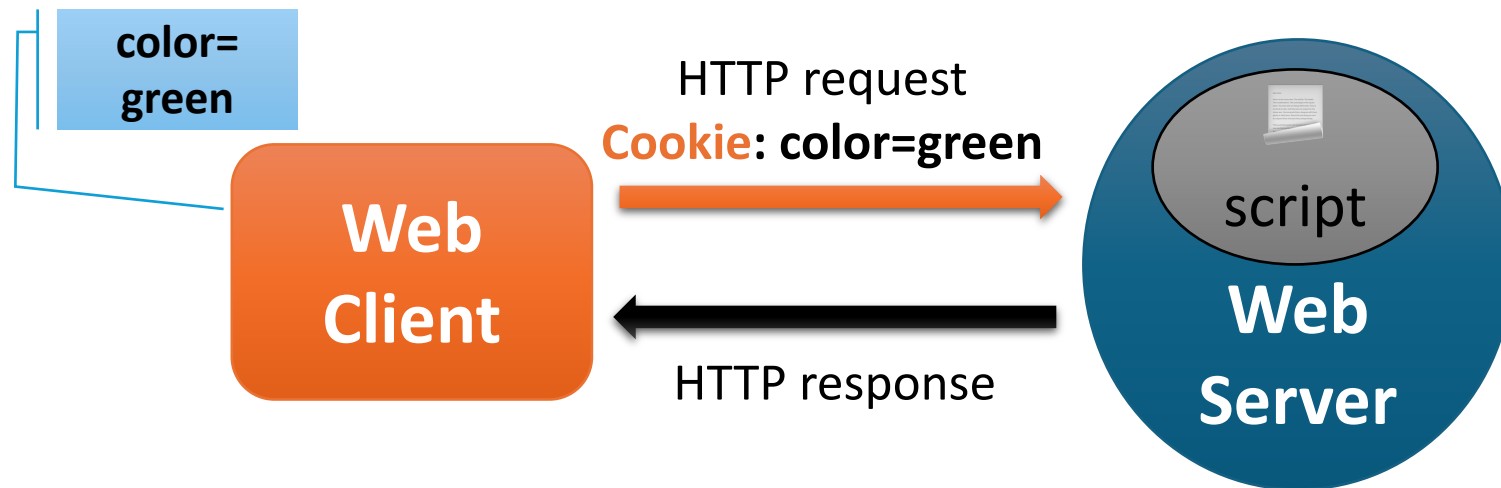
Cookies – persistent or not –
are processed and stored by the browser



persistent cookies are stored in files or databases (SQLite)

Cookies

Next access to the script is made by transmitting the cookies to the server according to the validity conditions



Cookies – Consulting

Cookies reside in the header field
of an HTTP message

Cookies – Expiration

To remove a cookie,
the value and time are canceled

eventually, the other attributes of the cookie

Cookies – Expiration

advanced

Other information of interest is available in
RFC 6265

HTTP State Management Mechanism

datatracker.ietf.org/doc/html/rfc6265

How can we identify successive requests expressed by the same client instance?

Behavior

HTTP is a **stateless** protocol

Behavior

HTTP is a **stateless** protocol

does not offer information if certain successive requests
are received from the same client
(from the same instance of a Web browser)

Sessions

Each visitor of a website will have associated
a unique identifier – **session ID (SID)**

stored by a cookie

(e.g., ASP.NET_SessionId, JSESSIONID,
PHPSESSID, session-id, _wp_session)

or

propagated via an URL

Sessions

Each visitor of a website will have associated
a unique identifier – **session ID (SID)**

in this way, consecutive visits (requests) made by
the same user can be identified

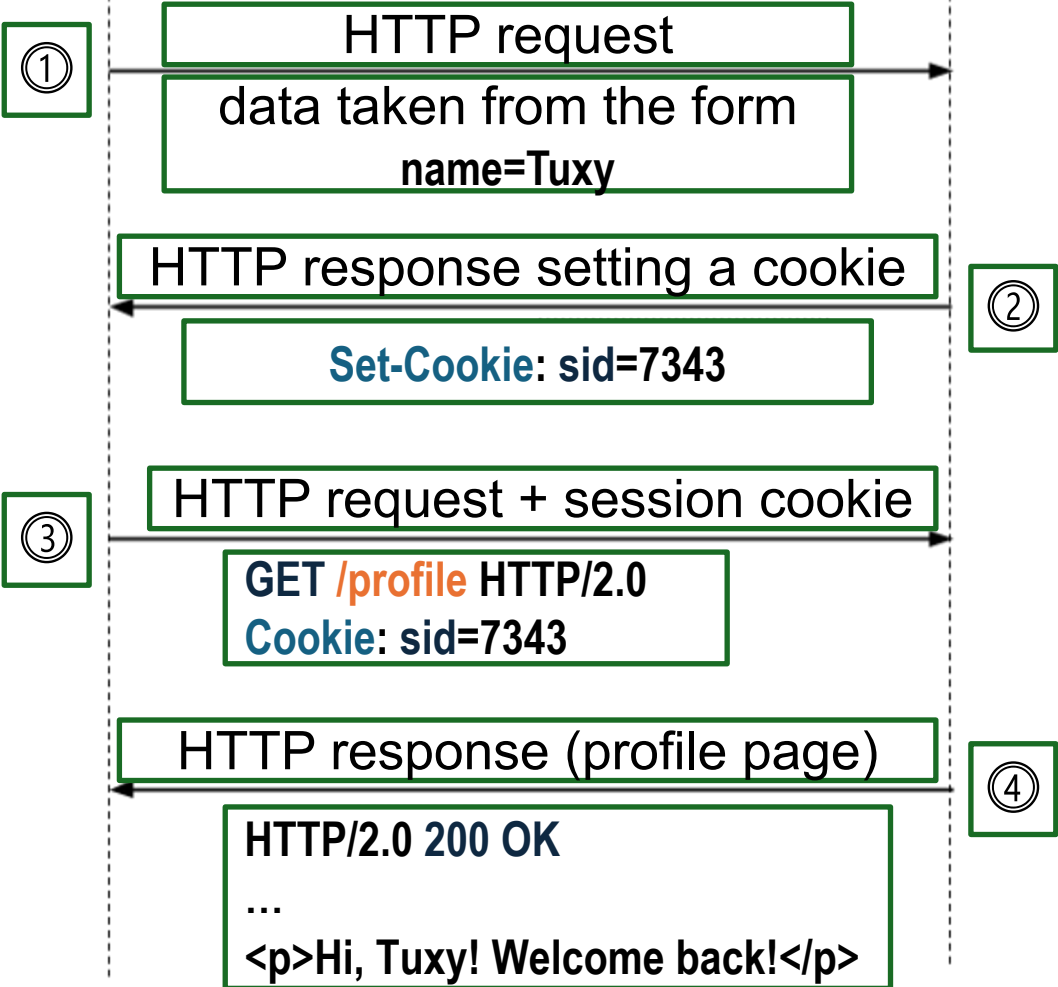
Sessions



Web client (browser)

Web server

establishing a
Web session
using a cookie



Sessions

advanced

Various variables can be attached to a session

their values will be kept (stored) between consecutive
– e.g., related – requests from the same instance
of a Web client (browser)

Sessions

advanced

A session could be implicitly (automatically) or explicitly (manually, by programmer) registered, depending on the Web application server or the default configuration

Sessions

advanced

A session could be implicitly (automatically) or explicitly (manually, by programmer) registered, depending on the Web application server or the default configuration

Web session info is persistently stored on the server by using non-relational database systems – e.g., DynamoDB, Memcached, Redis,... – or, in most cases, files

Sessions

POST / HTTP/1.1

Accept: text/html,application/xhtml+xml,
application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en,en-GB;q=0.5

Connection: keep-alive

Cookie: language=en_US

Host: mail.info.uaic.ro

Referer: https://mail.info.uaic.ro/?_task=login

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 ... Gecko/20100101 Firefox/144.0

user authentication by using the POST method
(already existing cookies are transmitted)

Sessions

```
HTTP/1.1 302 Found
Cache-Control: private, no-cache, no-store, must-revalidate...
Connection: Keep-Alive
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Fri, 31 Oct 2025 10:18:32 GMT
Keep-Alive: timeout=5, max=100
Last-Modified: Fri, 31 Oct 2025 10:18:32 GMT
Location: ./?\_task=mail&\_token=cb1924...c9c97819
Server: Apache
Set-Cookie: roundcube_sessid=vnqrt4...2uv2; path=/; HttpOnly
Set-Cookie: roundcube_sessauth=S92ee64...2c71; path=/; HttpOnly
```



redirection after authentication

HTTP response
a Web session-related cookie is set

Sessions – Example (pocket)

advanced

a95b4b6: "6b3gdd4bpb671A4094TqK53T54A1pf8a737X0xV0V3yRb7gM409b8u80F74ZW140"

ab.storage.deviceId.4fee55ff-f105-4a61-843b-856c583b109e: '{"g": "401b326f-8570-156b-f9fc-7d4bbb000773", "c": "1676700335923", "l": "1677577074716"}'

ab.storage.sessionId.4fee55ff-f105-4a61-843b-856c583b109e: '{"g": "e731ea6e-6683-3e8b-94d5-cc3cf41820c7", "e": "1677578874716", "c": "1677577074716", "l": "1677577074716"}'

ab.storage.userId.4fee55ff-f105-4a61-843b-856c583b109e: '{"g": "6b3gdd4bpb671A4094TqK53T54A1pf8a737X0xV0V3yRb7gM409b8u80F4ZW140", "c": "1676700335922", "l": "1677577074716"}'

AUTH_BEARER_default: "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiJ9.eyJpYXQiOiJlZ2Nzc1NzcvNzUzLWV0V3yRb7gM409b8u80F74ZW140", "c": "1676700335922", "l": "1677577074716"}"
BEZIIUK0xDXC9IcFI0WUlxVMza21kaklBPSlslmzlcy16lmdldHBvY2tldC5jb20iLCJuYmYiOiJlZ2Nzc1NzcvNzUzLWV0V3yRb7gM409b8u80F74ZW140", "e": "1677578874716", "c": "1677577074716", "l": "1677577074716"}"
MTY3NzU4MDY3NSwiZGF0YSI6Ij9.eyJpYXQiOiJlZ2Nzc1NzcvNzUzLWV0V3yRb7gM409b8u80F74ZW140", "e": "1677578874716", "c": "1677577074716", "l": "1677577074716"}"
8KJAOJN2Y3-HszY_pbaRZkNDPD8-oTnMfj9DVAjW1Kd18upOnWj9u_bjNUWL6LNpbVW600Lm3-lba2AaYY2G_H0HO_dv8f-ReG2f3-p966H3VzNtm5QSrrOGMxv6gMYfm9HCLprxfc3jMPrrn...
hzJZhaJi44R_jAJPUvNRPf_WCCJI0FrdWre6KQYNAAj6ywgabgn...
7qPD5g65cUtfLYO_4D5C4ZdERw"

various cookies associated with the current Web session: authentication information, user identifier, different options, ...

d4a79ec: "8049dae93dc1360de07ff30ed0bfc147190d3c76fb8b098da37d99fbdc1d8aa6"

fsv1: "6f0c35c3f262a843ee3ed4ff2869387bd5d2df9d"

ftv1: "cd8ecd2d-0780-0f2d-65e5-523768"

OptanonConsent: "isIABGlobal=false&datestamp=Sat+Feb+18+2023+08:05:23+GMT+0200+(Eastern+European+Standard+Time)&version=6.14.0&hosts=&consentId=f5917bde-d4c4-4198-b372-e089a9e2ae2e&interactionCount=1&landingPath=NotLandingPage&groups=C0001:1,C0002:1,C0004:0&AwaitingReconsent=false"

PHPSESSID: "383abc47abb9c955bbca3caf2091a323"

ps: "0"

sess_guid: "4aNT4A17gzd79ZbTh0d8411B30p4y86501ec31H670F261f246a73Yc4v36yY353"

Sessions – Programming

advanced

In the case of CGI, session management must be entirely implemented by the programmer

there is no standard way for Web session management

Alternatives

advanced

Web Storage

browser-level storage for lists of key—value pairs
via **sessionStorage** and **localStorage** attributes

see HTML Living Standard (4 Nov. 2025) specification
html.spec.whatwg.org/multipage/webstorage.html

developer.mozilla.org/en-US/docs/Web/API/Web_Storage_API



Summary